REMARKS

The Non-Final Office Action mailed June 16, 2010, considered and rejected claims 24, 25, 27, 28, 34, 36-38 and 40-45. Claims 24 and 34 were objected to because of informalities corrected by this amendment[1]. Claims 34, 38, 40-43, and 45 were rejected under 35 U.S.C. § 101 because the claimed invention was directed to non-statutory subject matter. Claims 24, 25, 27, 28, 34, 36-38, and 40-45 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Glasser* (US 6,061,684) in view of *Nowicki* (US 7,146,377).[2]

By this paper, claims 24 and 34 are amended, claims 46 and 47 are added, and no claims are cancelled.[3] Accordingly, following this paper, claims 24, 25, 27, 28, 34, 36-38 and 40-47 remain pending, of which claims 24 and 34 are the independent claims at issue.

As reflected above, the claims are generally directed to zone based security administration for data entities. For example, claim 24 recites a method of authenticating principal identity and then splitting the one or more non-overlapping security zones into a plurality of non-overlapping security zones to facilitate more efficient delegation of rights to principals. As part of such method, a first access control list (ACL) is accessed, the first ACL defining administrative rights based on common security rules that principals are to have in an existing non-overlapping zone from among the one or more non-overlapping zones. Authentication information is accessed that that specifies the identity of the principals that are to have the administrative rights in the existing non-overlapping zone. Claim 24 further recites authenticating the principals by verifying the identity of the principals by using the authentication information and by verifying that the principals are to have the administrative rights defined in the first ACL.

A grouping of data items and method items in the combined item hierarchy for which new common security rules are to be enforced is identified. The identified grouping of data items and method items are currently included in the existing non-overlapping zone from among

---

[1] In particular, the Office objected to the plural "zones" in the phrase "the new non-overlapping security zones," while only a single new-non-overlapping security zone is previously recited. Applicant notes that the body of the claim now recites "zone" in the singular in such phrase. Accordingly, Applicant respectfully submits that the objection is overcome.

[2] Although the prior art status of the cited art is not being challenged at this time, Applicant reserves the right to challenge the prior art status of the cited art at any appropriate time, should it arise. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status of the cited art.

[3] Support for the claim amendments and new claims can be found throughout the originally filed application, including at least the disclosure in paragraphs 35-38 and 41, as numbered in the application as filed, as well as in the original claims and figures.

the one or more non-overlapping zones. Existing common security rules are enforced within the existing non-overlapping zone and the new common security rules differing from the existing common security rules. A processor re-configures the one or more non-overlapping security zones so that rights can be delegated at a granularity that is finer than an entire database but yet coarse enough so as to not require delegation for each item. Re-configuring includes splitting the existing non-overlapping security zone into a new non-overlapping security zone and a remnant of the existing non-overlapping security zone. The arrangement of the new non-overlapping security zone relative to the remnant of the existing non-overlapping security zone is based on the location of the identified grouping of data items and method items within the combined item hierarchy. The new non-overlapping security zone is for containing the identified grouping of data items and methods items. The remnant of the existing non-overlapping security zone contains at least one data item or method item from the existing non-overlapping security zone. Accordingly, splitting is restricted in such a way as to prevent overlapping between security zones and such that none of the data items and method items is included in more than one security zone. Re-configuring also includes adjusting data properties of each of the items in the identified grouping of data items and method items to represent that the identified grouping of data items and method items are contained in the new non-overlapping security zone.

For any principals that had existing rights in the existing non-overlapping security zone based on the existing common security rules being enforced in the existing non-overlapping security zone at the time the existing non-overlapping zone was split, those rights are retained. Thus, the rights are retained in the identified grouping of data items and methods items, subsequent to splitting the existing non-overlapping security zone and subsequent to adjusting data properties to represent that the identified grouping of data items and methods items are contained in the new non-overlapping security zone. Other rights in the new non-overlapping security zone are identified and granted to one or more additional principals in accordance with the new common security rules, and after splitting of the existing non-overlapping security zone into the new non-overlapping security zone and the remnant of the existing non-overlapping security zone. Assigning the other rights to the new non-overlapping zone collectively grants the other rights to each item in the identified grouping of data items and method items through the assignment of the other rights to the new non-overlapping security zone. The other rights differ from the existing rights.

Claim 34 is a computer program product claim corresponding to the method of claim 24. Claim 47 is a method related to the method of claim 24, in which a security zone is split and a new zone is created with no initial security rules, such that all security rules are created for the new zone after creation of the zone.

1. Rejections under 35 U.S.C. § 101

As noted above, claims 34, 38, 40-43 and 45 were rejected as being directed to non-statutory subject matter. Applicant respectfully traverses.

In particular, it will be noted that the Office states that the recited computer program product that includes "one or more computer-readable storage media" includes as a definition the use of a signal, such that the media can be interpreted to include media. (Office Action, p. 4). The entire basis for such statement appears is a statement that Applicant's specification describes computer-readable storage media in an open-ended manner using examples.

Applicant respectfully submits that the use of examples to describe an element does not mean that the described component can encompass any other element, however unrelated to the provided examples. In Applicant's specification, it is worthwhile to view the examples provided in describing "computer-readable storage media." In particular, Applicant's specification states that "computer-readable media" can include RAM, ROM, EEPROM, CD-ROM or other optical, or magnetic disk storage devices, or any other medium that can carry or store program code. (¶ 59). The Application then further describes a connection as a "computer-readable medium." (*Id.*). By way of additional description, the specification states that "computer readable media for storing data can [include] magnetic cassettes, flash memory cards, digital versatile disks, Bernoulli cartridges, RAMs, ROMs, and the like." (¶ 63).

Accordingly, Applicant's specification describes "computer-readable media" as including effectively two types, namely storage-type media and carry or communication-type media. Each time storage-type media is described, physical examples (e.g. magnetic, optical, flash, etc) of devices are used to describe the storage media. At no point is storage media described as including any example of a signal, connection, or other communication-type media. The Office has apparently used the discussion "computer-readable media" and made such equally applicable to "computer-readable storage media" when such is the case. "Storage" media is clearly a subset of computer-readable media, and clearly excludes signals inasmuch as signals carry, rather than

store, code means. Although not believed necessary in view of the clear differentiation of "storage" vs. "communication" type media, Applicant expressly disclaims any coverage in claims 34, 38, 40-43, and 45 to the extent "computer-readable storage media" could be interpreted to require only a single without any additional physical, article of manufacture.

In view of Applicant's description of "storage" media as opposed to merely "computer-readable media," and the express disclaimer herein, Applicant respectfully submits that claims 34, 38, 40-43 and 45 are clearly directed to statutory subject matter.

2. Rejections under 35 U.S.C. § 103

While the cited art generally relates to controlling user access to a resource in a networked environment and/or partitioning metadata of a storage system, Applicant respectfully submits that the cited art, whether such references are cited individually or collectively, fails to render the pending claims unpatentable. For instance, among other things, Applicant respectfully submits that the cited art fails to disclose, suggest, or reasonably support each and every element of the pending claims.

In particular, *Glasser* teaches a unified and straightforward approach to managing file and other resource security in a networked computing environment. A resource is organized as a hierarchy of elements with a root element at the top of the hierarchy and additional elements below the root element. In such a system, a resource is selected and a command is received to change the permissions for the selected resource. Thereafter the resource access permissions are changed and propagated to children of the resource in a hierarchy, and registry records are updated with the new permissions. (Col. 7, ll. 54-64). More particularly, a user interface is used such that when a resource is selected, the ACL for that resource is displayed on the user interface. The displayed ACL will correspond directly to the selected resource if the resource has its own ACL, or will correspond to the nearest ancestor having an ACL if no ACL is specific to the selected resource. (Col. 7, ln. 65 to Col. 8, ln. 9).

Once the ACL is displayed, a user can select to add or remove users identified in the ACL, or to alter the permissions of the users listed in the ACL. (Col. 8, ll. 10-36). Upon selecting the changes, a command button is pressed to issue a command that causes the peer server to process the changes. (Col. 8, ll. 36-39). The peer server generates a list of changes and then merges the changes into the ACL corresponding to the resource, by either changing the

existing ACL or causing a new ACL to be created. (Col. 8, ll. 55-66). The changes apply directly to descendents not having their own ACLs, and changes can also be selectively propagated down to other descendants in the resource hierarchy that do have their own ACLs (Col. 9, ll. 4-57).

Nowicki teaches a metadata management system (MDS) that may include partitioned migratable metadata. Metadata may be stored in multiple metadata partitions (102-0 to 102-11). Each metadata partition may be assigned to a particular system resource (104-0 to 104-5). According to predetermined policies, such as metadata aging, metadata stored in one metadata partition may be migrated to a different metadata partition. A forwarding object can be placed in the old metadata partition to indicate the new location of the migrated metadata. Metadata partitions (102-0 to 102-11) may be reassigned to different resources, split and/or merged allowing a high degree of scalability, as well as flexibility in meeting storage system needs.

Accordingly, while *Glasser* and *Nowicki* collectively teach assigning different security protections to different folders/resources, and using metadata partitions that can be realigned between resources, the cited art fails to disclose or reasonably support the pending claims. For instance, among other things, the cited art fails to disclose or reasonably support that identification and/or granting of administrative rights in a new non-overlapping zone after the previously existing zone is split, as such is recited in combination with the other claim elements. Indeed, the combination of *Glasser* and *Nowicki* teaches the direct contrary. In particular, a "zone" in *Glasser* does not appear to be split until a resource with inherited permissions has a different set of permissions are applied. If no new permissions are applied, the permissions are still obtained by inheritance such that a separate zone would be overlapping, rather than non-overlapping. More particularly, splitting a zone occurs in *Glasser* by initially selecting a change to a resource permission, and then applying the change to create the new zone. In direct contrast, the pending claims generate permissions after the zone is created, rather than identifying and generating changed permissions as a first instance. Indeed, inasmuch as selecting the permission change is the impetus for "zone" creation in *Glasser*, and the basis on which the user interface and software work, there would be no reason to modify such teaching and it would change the operative principle of *Glasser*. Furthermore, as *Nowicki* relates to metadata partitions, but Applicant has not identified any disclosure relevant to changing security permissions, let alone

splitting zones prior to modifying security permissions. As such, *Nowicki* fails to remedy the deficiencies of *Glasser*.

In view of the foregoing, Applicant respectfully submits that the other rejections to the claims are now moot and do not, therefore, need to be addressed individually at this time. It will be appreciated, however, that this should not be construed as Applicant acquiescing to any of the purported teachings or assertions made in the last action regarding the cited art or the pending application, including any official notice.[4] Instead, Applicant reserves the right to challenge any of the purported teachings or assertions made in the last action at any appropriate time in the future, should the need arise. Furthermore, to the extent that the Examiner has relied on any Official Notice, explicitly or implicitly, Applicant specifically requests that the Examiner provide references supporting the teachings officially noticed, as well as the required motivation or suggestion to combine the relied upon notice with the other art of record.

In the event that the Examiner finds remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney at (801) 533-9800.

Dated this 2nd day of November, 2010.

Respectfully submitted,

/Colby C. Nuttall, Reg. No. 58,146/
Colby C. Nuttall

RICK D. NYDEGGER
Registration No. 28,651
COLBY C. NUTTALL
Registration No. 58,146
Attorneys for Applicant
Customer No. 047973

RDN:CCN:crb
2930633_1

[4] For instance, the independent and dependent claims include various other elements not taught, suggested, or reasonably supported by the art of record. For instance, claim 47 recites that a new non-overlapping zone has rights associated therewith, and isolated from the other non-overlapping zones. In contrast, *Glasser* specifically notes that when a new right is added and a new zone created, descendents that have their own ACLs (and thus own zones) are also evaluated such that the rights can be passed thereto. Accordingly, new rights are propagated to other zones based on the change, such that changes are not isolated with respect to other zones.